Wi-Fi Predators
by Zen II Net

Whether you are a "pro" with your PC or only perform the basics (checking your e-mail, reading the news, finding a flight or hotel, etc.), today's technology has led us to enjoy more and more the freedom from networking cables. This means that our phones, music devices and computers (laptop, notebook) depend on wireless connections to access the internet world. That´s great – it makes our lives easier and we love the freedom it gives us!

But unfortunately there lurk those "baddies" whose main purpose is to invade our private lives, steal our passwords, user names, email messages, account numbers, other personal information, learn where we live, and perhaps even steal our identities. Other than these types, there are the "cyber vandals" – the people who just want to see what mischief they can achieve. The terms "hacking", "virus", "malware (up to 30,000 new threats are created every day)", and "Trojan" apply more than ever today as we depend increasingly on wireless networks; some cities have major geographical areas available with free Wi-Fi connections, as do many public libraries, coffee shops, restaurants, and of course airports. Recent publicized studies have proven that a wireless network could be hacked in less than 5 seconds.....and it doesn't take a genius to figure out how to do it either. In fact, it was also recently reported that Spain has more hackers than any other EU country, but today you can be vulnerable anywhere in the world. There are many software programs available and tutorials on the internet that allow the user to be able to hack into anyone's system.

The problem is that many people trust that their wireless network is safe; the same aforementioned study showed that 82% of the 40,000 Brits tested thought their network was safe and used it without password protection. Hackers have been known to "harvest" usernames and passwords at an alarming rate of more than 350 per hour by simply sitting in a coffee shop or restaurant in a busy city. Those free "Wi-Fi networks" or "Hotspots" are often unencrypted, employ a wireless router that broadcasts all communications between itself and those connected computers. This means that if there are 15 people on their laptops, reading their mail, downloading music, chatting or just surfing the net, all those 15 people's communications are being broadcast and shared throughout the immediate area. By using a non-protected wireless network, the individual private user is open to eavesdropping, hacker attacks and to being used by others for illegal activities. We have already heard about numerous people whose identities were stolen, whose bank accounts emptied, credit cards used, and who had been accused of being involved in illegal activities such as child pornography, selling stolen goods and human trafficking. This is not movie fodder but real life, and it happens in every country. (In our own business, we have had several cases of clients whose computers have been compromised, requiring major or minor repairs, freezing of their bank accounts, or a complete refurbishing of their operating system.) So if your laptop or notebook has recently slowed down considerably or is misbehaving, think about where you have used it in the recent past.....you may have an unwelcome visitor or perhaps have been hacked into.

There are, of course, some ways to protect yourself from these dangers. Some people may think it inconvenient, time-consuming or costly, but in the long run may well be worth the effort.

- Use a router and an ethernet cable for all your internet connections, especially when using the internet on sites that require your login and transfer of personal data (e.g. online banking, using your credit card to shop or buy airline tickets, chatting on social network sites). A router which has its own firewall provides an external IP address thereby leaving your computer on an internal IP, thus preventing a hacker from accessing your computer when scanning. Remember to keep it updated from the

manufacturer as part of your automatic updates. Use a router with high security from a reliable company such as *D-Link, Belkin, Netgear, Linksys*, etc. (We have always reiterated to our clients to never skimp on connection quality, security and memory of their computer systems.)

- Keep your operating system updated – Microsoft, Mac, and Linux frequently issue updates to your computer's security system so don't ignore those messages when they appear on your screen – download and install them immediately.

- Use the firewall that came with your operating system – it's there for a good reason, as it requires your permission to install any software that it does not recognize.

- When creating passwords for your computer and/or wireless network connection setup, make them difficult. Use letters, numbers and even symbols. They should be at least 20 characters long and be uncommon alphanumeric combinations - **never** use your personal information, such as phone numbers, birth date, children or mate's name, and other obvious information. The more complicated and distinct from you, the better. Remember to write the password somewhere lest you forget, but store that note in a safe place, away from the computer.

- If you are on a wireless network, at the present time you should select WPA or WPA2 security, as opposed to WEP protocol (older and can be easily broken into). As newer routers arrive on the market, the better the security protection will be so you should adjust your system accordingly.

- If you are one of the approximately 95% of the world using "Windows" systems, then you must install a very good internet security/anti-virus program. These are not free, as the free versions tend to overlook many aspects during their scans; some only let you know there is a problem but do not **fix** it. This is as important an investment as your computer was so get the most comprehensive software possible (that means everything from your hard drive to e-mails are protected, your system is continuously updated in real time, etc.) If you cannot decide which program is the best for you, be aware that reputable software providers will let you download and use their program free for 30 days prior to purchasing.

- "Windows" users love their mail manager, Outlook Express. However, it is not the safest way to access your mail. Using the web is far better, as email companies such as Gmail, Yahoo and Hotmail have extremely high security levels on their sites. Yes, it's much simpler to go to one place (i.e. Outlook) to get your mail, but Gmail and others have begun to provide similar functions to their account holders.

- Beware of links within your email. Hackers have been known to successfully clone company logos, design and terminology (e.g. PayPal), where the user thinks he/she is accessing PayPal when in reality they are divulging their bank information and other personal data to a hacker. A good rule of thumb is if you are dealing with personal data and money, log onto the original website and sign in there to conduct your business.

- Take care with the sharing of your hard drive on your home network. It's best to share a folder or folders, not your entire drive, in the event you become a hack victim.

- Make sure that the websites you visit that require your personal information use SSL-encryption, particularly if you are using your laptop in a public place. Look for the padlock icon in front of the web address or "https" in the address bar – the "s" signifies that the site is secure and protected as it uses "point-to-point" or "P2P" encryption. This type of encryption is automatically installed when you visit the site;

thus your browser encrypts all data that it sends before it leaves your PC, decrypting the information only when it reaches its destination website, and vice versa. Shopping-cart sites, online banking and other responsible sites that request your personal information use this type of encryption.

- Last but not least, be observant when using your laptop in a public place without encrypted security. If you choose to do your banking, read your mail, or pass along other sensitive information, be aware of others near you who are on their own laptops. Hackers know that users of public Wi-Fi areas (sometimes as far as 300 mtrs. away) are easy targets for them. It is the same as giving a stranger the keys to your house and walking away.

- Social networking sites grow in popularity daily but so does the user´s vulnerability. The combination of wireless connection and sharing of private information on these sites can be an open door for unpleasant situations, so use caution when sharing your news.

The gravity of hackers has once again been publicized. Take a look at this report. Click on:

http://news.yahoo.com/s/ap/20101122/ap_on_re_us/us_cybercrime_money_mules

or search Yahoo News for the Article entitled "Cyberthieves still rely on human foot soldiers."

The PC and all our wonderful handheld devices are signs of our global growth – who knows what kind of devices we will be using 5 years down the road! We just have to remember that the more connected we become – virtually speaking – the more we become available, and vulnerable too. We just need a good suit of armor!